Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for securely controlling the printing of a plaintext document generated by a first source, the method comprising the steps of:

receiving at a printer via a first communication channel a first key sent by the first source;

obtaining at the printer a second key based on communication between the printer and a second source;

receiving at the printer from the second source via a second communication channel an encrypted version of the plaintext document that cannot be decrypted at the second source to obtain the plaintext document;

decrypting at the printer using the first and second keys the encrypted version of the plaintext document to obtain the plaintext document at the printer; and

printing with the printer the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document;

wherein the second communication channel is an electronic communication channel.

2. (Canceled)

3. (currently amended) A method as recited in claim 12, wherein the second communication channel is a secure electronic communication channel.

4. (currently amended) A method as recited in claim 12, wherein the second communication channel is a non-secure electronic communication channel.

5. (cancelled)

6. (currently amended) A method as recited in claim 15, further comprising the step of ensuring that the printer can only print a predetermined number of copies of the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document.

7. (original)A method as recited in claim 6, wherein the predetermined number is one.

8. (original) A method as recited in claim 7, further comprising storing in a memory in the printer the first and second keys, the encrypted version of the plaintext document, and the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document, and subsequent to the printing of the predetermined number of copies of the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document 1) deleting from the memory the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document and 2) deleting from the memory one of the first key, the second key, and the encrypted version of the plaintext document.

9. (original) A method as recited in claim 6, further comprising obtaining electronically at the printer the predetermined number from the second source.

10. (currently amended) A method as recited in claim 12, further comprising performing a first encryption operation on the plaintext document thereby creating an encrypted form of the plaintext document and subsequently performing a second encryption operation on the encrypted form thereby creating the encrypted version of the plaintext document.

11. (original) A method as recited in claim 10, wherein the first encryption operation is performed at the first source, the encrypted form is sent electronically from the first source to the second source, the encrypted form is stored at the second source, the second source does not have the ability to decrypt the encrypted form, and the second source performs the second encryption operation on the encrypted form.

12. (original) A method as recited in claim 11, wherein the second source is a server and the second key is generated at the server and sent to the printer via the second communication channel.

13. (original) A method as recited in claim 11, wherein the second source and the printer communicate to mutually agree on the second key.

14. (original) A method as recited in claim 6, wherein the second source maintains an audit record of the number of copies printed at the printer of the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document.

15. (currently amended) A method as recited in claim 12, further comprising printing the plaintext document obtained at the printer via the decrypting at the printer of the encrypted version of the plaintext document to include forensic evidence of the authenticity of the printed plaintext document.

16. (currently amended) A system for securely transmitting and printing documents comprising:

a computer system that encrypts a plaintext document using a first key thereby creating an encrypted document, the computer system including means for electronically transmitting the encrypted document via a first communication channel;

a server connected to the first communication channel to receive the encrypted document from the computer system, the server including memory for storing the encrypted document, a processor for encrypting the encrypted document using a second key thereby creating a double-encrypted document, means for electronically transmitting the double-encrypted document via a second communication channel;

a printer connected to the second communication channel, the printer having means for communicating with the server via the second communication channel to determine the second key and to receive the double-encrypted document from the server, means for receiving the first key from the computer system upon request, means for decrypting the double-encrypted document using the first and second keys to obtain the plaintext document, and means for printing a only a predetermined number of copies of the plaintext document obtained from the decrypting of the double-encrypted document by the printer;

wherein the server cannot decrypt the encrypted document to obtain the plaintext document.

17. (currently amended) A method for securely controlling the recording of an unencrypted digital content generated by a first source, the method comprising the steps of:

receiving at a recording device via a first communication channel a first key sent by the first source;

obtaining at the recording device a second key based on communication between the recording device and a second source;

receiving at the recording device from the second source via a second communication channel an encrypted version of the unencrypted digital content, the receiving device not being capable of decrypting the encrypted version of the unencrypted digital content;

decrypting at the recording device using the first and second keys the encrypted version of the unencrypted digital content to obtain the unencrypted digital content at the recording device; and

recording on a recording medium with the recording device the unencrypted digital content obtained at the recording device via the decrypting at the recording device of the encrypted version of the unencrypted digital content.